

Rec'd PCT/PTO 29 APR 2005

#2

PCT/JP03/14055

10/533256

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

04.11.03

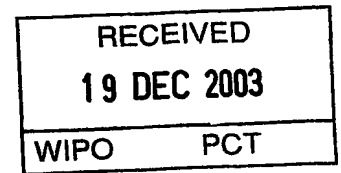
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2002年11月 1日

出 願 番 号  
Application Number: 特願2002-320035  
[ST. 10/C]: [JP2002-320035]

出 願 人  
Applicant(s): 三洋電機株式会社  
株式会社数理設計研究所  
三洋セミコンデバイス株式会社

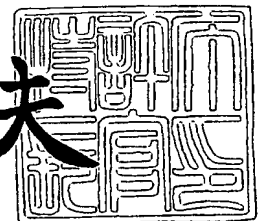


PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2003年12月 4日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特2003-3100239

【書類名】 特許願

【整理番号】 KGA1020075

【提出日】 平成14年11月 1日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/58  
G09C 1/00

【発明者】

    【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

    【氏名】 女屋 正人

【発明者】

    【住所又は居所】 群馬県前橋市上佐鳥町54-2 株式会社数理設計研究所内

    【氏名】 玉置 晴朗

【発明者】

    【住所又は居所】 東京都台東区上野1丁目19番10号 三洋セミコンデバイス株式会社内

    【氏名】 池谷 昭

【特許出願人】

    【識別番号】 000001889

    【氏名又は名称】 三洋電機株式会社

【特許出願人】

    【住所又は居所】 群馬県前橋市上佐鳥町54-2

    【氏名又は名称】 株式会社数理設計研究所

【特許出願人】

    【住所又は居所】 東京都台東区上野1丁目19番10号

    【氏名又は名称】 三洋セミコンデバイス株式会社

## 【代理人】

【識別番号】 100075258

【弁理士】

【氏名又は名称】 吉田 研二

【電話番号】 0422-21-2340

## 【選任した代理人】

【識別番号】 100096976

【弁理士】

【氏名又は名称】 石田 純

【電話番号】 0422-21-2340

## 【手数料の表示】

【予納台帳番号】 001753

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 乱数生成装置

【特許請求の範囲】

【請求項 1】 複数の異なる疑似乱数系列の乱数パターンを出力可能な疑似乱数生成手段と、

物理乱数を生成する物理乱数生成手段と、

前記物理乱数生成手段の生成した物理乱数に基づいて前記疑似乱数生成手段の出力する乱数の疑似乱数系列を切り替える切替手段と、

を備える乱数生成装置。

【請求項 2】 前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、

前記切替手段は、前記線形シフトレジスタ符号発生器への帰還入力値の反転／非反転を、前記物理乱数生成手段によって生成された物理乱数に基づいて切り替えることを特徴とする請求項 1 に記載の乱数生成装置。

【請求項 3】 前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、

前記切替手段は、前記線形シフトレジスタ符号発生器からの出力値の反転／非反転を、前記物理乱数生成手段によって生成された物理乱数に基づいて切り替えることを特徴とする請求項 1 に記載の乱数生成装置。

【請求項 4】 前記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、該線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく複数の帰還入力値を生成し、

前記切替手段は、前記生成された複数の帰還入力値のうち該線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、前記物理乱数生成手段で生成された物理乱数に基づいて切り替えることを特徴とする請求項 1 に記載の乱数生成装置。

【請求項 5】 前記疑似乱数生成手段は、所定のタップの組み合わせに基づく第一の帰還入力値を生成する線形シフトレジスタ符号発生器と、該第一の帰還入力値を受け取り前記線形シフトレジスタ符号発生器と同期して所定ビット数ビ

ットシフトを行いその出力を第二の帰還入力値とするフリップフロップと、を含み、

前記切替手段は、前記第一または第二の帰還入力値のうち前記線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、前記物理乱数生成手段で生成された物理乱数に基づいて切り替えることを特徴とする請求項 1 に記載の乱数生成装置。

【請求項 6】 請求項 2～5 のうちいずれか一つに記載の乱数生成装置であって、

前記線形シフトレジスタ符号発生器の符号列を検出する検出手段を備え、

前記切替手段は、有効な疑似乱数系列の乱数が前記検出された符号列によっては生成不能である場合には、該疑似乱数系列以外の疑似乱数系列に切り替えることを特徴とする乱数生成装置。

【請求項 7】 請求項 2～5 のうちいずれか一つに記載の乱数生成装置であって、

前記線形シフトレジスタ符号発生器の符号列を検出する検出手段と、

有効な疑似乱数系列の乱数が前記検出された符号列によっては生成不能である場合には、前記符号列のビット値のうち少なくとも一つを反転させることを特徴とする乱数生成装置。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、乱数生成装置に関し、特に暗号化アルゴリズムに好適な乱数生成装置に関する。

##### 【0002】

#### 【従来の技術】

暗号化アルゴリズム等では、セキュリティの確保のために、しばしば乱数が用いられる。その場合の乱数としては、一般的に、M系列 (Maximum length code : 最長符号系列) 等に代表される疑似乱数が用いられてきた。M系列符号は、公知の線形シフトレジスタ符号発生器によって生成することができる。

## 【0003】

また、上記疑似乱数以外の乱数として、原子核の崩壊現象がランダムとなることや電気雑音等の自然現象を利用して生成される物理乱数が知られている。暗号化アルゴリズム等においても、上記疑似乱数に替えて、この物理乱数を利用する場合もある（例えば、特許文献1参照。）

## 【0004】

## 【特許文献1】

特開 2000-66592 公報

## 【0005】

## 【発明が解決しようとする課題】

しかしながら、M系列等に代表される疑似乱数は、必ずしも安全性の高い乱数とは言えず、セキュリティ確保の面からは好ましくないところがある。疑似乱数は、一定の算術プロセスあるいは関数の組み合わせから生成されるため、同じ初期条件を与えれば同一の値となり、乱数の推定が可能となるからである。

## 【0006】

また、一般的に物理乱数は微弱な信号であるため、暗号化アルゴリズム等で使用するためには、通常、増幅器によって利用可能なレベルに増幅される。ところが、これら全体は電界や磁界によって影響を受ける場合があり、それらの意図的または意図せざる印加によって乱数の発生確率が操作され、安全性が低下してしまう場合があった。

## 【0007】

## 【課題を解決するための手段】

本発明にかかる乱数生成装置は、複数の異なる疑似乱数系列の乱数パターンを出力可能な疑似乱数生成手段と、物理乱数を生成する物理乱数生成手段と、上記物理乱数生成手段の生成した物理乱数に基づいて上記疑似乱数生成手段の出力する乱数の疑似乱数系列を切り替える切替手段と、を備える。すなわち、上記本発明にかかる乱数生成装置によれば、複数の異なる疑似乱数を物理乱数によって切り替えて出力するため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては

用いていないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

#### 【0008】

上記本発明にかかる乱数生成装置は、種々の形態によって実現することができる。例えば、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、線形シフトレジスタ符号発生器を含み、上記切替手段が、上記線形シフトレジスタ符号発生器への帰還入力値の反転／非反転を、上記物理乱数生成手段によって生成された物理乱数に基づいて切り替えるよう、構成することができる。

#### 【0009】

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段は、線形シフトレジスタ符号発生器を含み、上記切替手段は、上記線形シフトレジスタ符号発生器からの出力値の反転／非反転を、上記物理乱数生成手段によって生成された物理乱数に基づいて切り替えるよう、構成することができる。

#### 【0010】

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、線形シフトレジスタ符号発生器を含み、該線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく複数の帰還入力値を生成し、上記切替手段が、上記生成された複数の帰還入力値のうち該線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、上記物理乱数生成手段で生成された物理乱数に基づいて切り替えるよう、構成することができる。

#### 【0011】

また、上記本発明にかかる乱数生成装置は、上記疑似乱数生成手段が、所定のタップの組み合わせに基づく第一の帰還入力値を生成する線形シフトレジスタ符号発生器と、該第一の帰還入力値を受け取り上記線形シフトレジスタ符号発生器と同期して所定ビット数ビットシフトを行いその出力を第二の帰還入力値とするフリップフロップと、を含み、上記切替手段が、上記第一または第二の帰還入力値のうち上記線形シフトレジスタ符号発生器に帰還入力する帰還入力値を、上記物理乱数生成手段で生成された物理乱数に基づいて切り替えるよう、構成するこ

とができる。

#### 【0012】

また、上記本発明にかかる乱数生成装置では、上記線形シフトレジスタ符号発生器の符号列を検出する検出手段を備え、上記切替手段は、有効なまたは切り替えによって有効となる疑似乱数系列の乱数が上記検出された符号列によっては生成不能である場合には、該疑似乱数系列以外の疑似乱数系列に切り替えるのが好適である。これにより、線形シフトレジスタ符号発生器において有効な疑似乱数系列に対して疑似乱数の生成されない符号列となるのが抑制される。

#### 【0013】

また、上記本発明にかかる乱数生成装置では、上記線形シフトレジスタ符号発生器の符号列を検出する検出手段と、有効なまたは切り替えによって有効となる疑似乱数系列の乱数が上記検出された符号列によっては生成不能である場合には、上記符号列のビット値のうち少なくとも一つを反転させるのが好適である。このような構成によっても、線形シフトレジスタ符号発生器において有効な疑似乱数系列に対して疑似乱数の生成されない符号列となるのが抑制される。

#### 【0014】

##### 【発明の実施の形態】

実施の形態1. 図1は本実施形態にかかる乱数生成装置10の構成図、図2は乱数生成装置10によって生成される二つのM系列の巡回パターンを示す図、また図3は物理乱数発生器14の構成図である。

#### 【0015】

乱数生成装置10は、疑似乱数生成部12、物理乱数発生器14、および切替部16を含む。このうち疑似乱数生成部12は、少なくとも一つの線形シフトレジスタ符号発生器を含み、複数の異なる疑似乱数系列（例えば、M系列等）の乱数パターンを出力することができる。本実施形態では、縦続して接続された複数のフリップフロップを含むシフトレジスタ18と、所定の複数のタップ位置からの出力値の排他的論理和を出力するEXORゲート20と、が設けられており、これらにより、M系列の乱数を出力する線形シフトレジスタ符号発生器が構成されている。図1の例では、シフトレジスタ18は、17個のフリップフロップを

有しクロック（CK）に応じてビットシフトする17段シフトレジスタとして構成され、入力側より第3番目と第17番目のフリップフロップからのタップ出力（Q出力；Q3，Q17）に基づいて帰還入力値（シフトレジスタ18のD1入力；「1」（ハイレベル）または「0」（ローレベル））が生成される。

#### 【0016】

一般的な線形シフトレジスタ符号発生器では、EXORゲート20の出力がそのままシフトレジスタ18に帰還入力されるが、本実施形態では、EXORゲート20の出力は切替部16を経由してシフトレジスタ18に入力される。切替部16は、物理乱数発生器14からの物理乱数出力（バイナリコード）に基づいて、帰還入力値となるEXORゲート20からの出力値の反転／非反転を切り替える。すなわち、この物理乱数出力は、切替制御信号とすることができる。図1の例では、切替部16は、EXORゲートとして構成される。EXORゲートは、二つの入力値が不一致であるときに「1」を出力し、一致するときに「0」を出力する。したがって、物理乱数出力値が「1」であるときは、切替部16においてEXORゲート20の出力値は反転され、他方、物理乱数出力値が「0」であるときは、反転されない。つまり、切替部16は、物理乱数出力値に応じて、EXORゲート20からの出力値を反転して帰還入力値とするか、あるいは反転させずにそのまま帰還入力値とするかを、切り替えていることになる。

#### 【0017】

このような切替部16の動作により、疑似乱数生成部12は、異なる二つの疑似乱数系列を生成することができる。図1の例では、物理乱数出力値が「0」であるときは切替部16において帰還入力値は反転されないから、疑似乱数生成部12においてクロック信号（CK）に基づいて $2^{17}-1$ サイクルで循環的に変化するM系列1-1（図2（a））が生成され、他方、物理乱数出力値が「1」であるときは、切替部16において帰還入力値が反転されるから、同じくクロック信号に基づいて $2^{17}-1$ サイクルで循環的に変化するM系列1-2（図2（b））が生成される。なお、M系列1-1とM系列1-2とは、変化のパターンは同一であるが、符号が互いに逆となっており、異なる疑似乱数系列として取り扱うことができる。これにより、切替部16に与える切替信号が物理乱数で制御されるの

で、一方の疑似乱数系列を生成するシフトレジスタの途中情報を用いて、他方の疑似乱数系列から一方の疑似乱数系列に切り替えることにより、予測不可能な疑似乱数系列となる。また、二つの疑似乱数系列の「0」と「1」の頻度がそれぞれ $2^{16}-1$ および $2^{16}$ と、 $2^{16}$ および $2^{16}-1$ の対称比率になるので、二つの疑似乱数系列を物理乱数によって切り替え制御すれば、「0」と「1」の頻度分布状態が理想状態に近づくという効果もある。

#### 【0018】

図3に示すように、物理乱数発生器14は、物理乱数発生源14a、増幅回路14bおよび二値化回路14cを備える。このうち、物理乱数発生源14aは、自然現象に基づいてランダムに変化する信号を生じうるものであり、例えば、上記特許文献1に開示されるような、接合を含む電流路に生じる雑音信号を生じる半導体素子を含むものとすることができる。なお、これには限られず、放射性物質の崩壊を利用したもの等もこの物理乱数発生源14aとして用いることができる。物理乱数発生源14aにて生じた信号は、増幅回路14bにおいて増幅され、さらに二値化回路14cにおいて二値化処理される。二値化回路14cは、所定のサンプリングタイミングで、増幅された信号の振幅と所定の閾値とを比較し、例えば、増幅された信号の振幅が所定の閾値より高いときには「1」を、逆に低いときには「0」を出力する。こうして物理乱数発生器14により、「1」または「0」を示す所定電圧の物理乱数出力値が生成される。なお、二値化回路14cにおける閾値のレベルは任意に設定することができるが、通常は「1」および「0」の発生確率がほぼ1対1となるように設定される。なお、二値化回路14cにおいて、単に、増幅された信号の振幅を所定の閾値と比較して出力信号を発生するようにしてもよい。

#### 【0019】

このように、本実施形態にかかる乱数発生装置10では、二つの異なる疑似乱数系列のうちどちらを出力するかを、物理乱数によって切り替えるだけでなく、シフトレジスタの途中情報を有効に利用して二つの疑似乱数系列の帰還状態を変化させている。こうすることで、疑似乱数のみを用いた場合に比べて、乱数の予測が難しくなる。また、物理乱数を直接的な出力乱数としては用いないため、

仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

#### 【0020】

実施の形態2. 図4は本実施形態にかかる乱数生成装置30の構成図である。乱数生成装置30は、疑似乱数生成部32、物理乱数発生器14、および切替部36を含む。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0021】

本実施形態にかかる疑似乱数生成部32では、線形シフトレジスタ符号発生器からの出力値を、切替部36によって反転または非反転して出力乱数とする。図4の例では、シフトレジスタ18およびEXORゲート20を含む典型的な線形シフトレジスタ符号発生器が構成されており、シフトレジスタ18の所定ビット（例えば第17番目のビット）のQ出力およびQb出力（Q出力の反転出力）がそれぞれ切替部36に入力される。

#### 【0022】

切替部36は、二つのANDゲート36a, 36bを備えており、そのうち一方のANDゲート36aには、Qb出力と物理乱数発生器14からインバータ36cを介して物理乱数出力が入力され、もう一方のANDゲート36bには、Q出力と物理乱数発生器14からの物理乱数出力が入力される。そして、これら二つのANDゲート36a, 36bの出力がORゲート36dに入力され、このORゲート36dの出力が出力乱数となる。

#### 【0023】

この切替部36により、物理乱数出力に応じてQ出力あるいはQb出力のうちいずれか一方が有効となる。すなわち物理乱数出力値が「1」のときは、ANDゲート36aの出力値は必ず「0」となり、かつANDゲート36bの出力値はQb出力値と同じになるので、乱数出力値はQb出力値と同じになる。逆に物理乱数出力値が「0」のときは、ANDゲート36bの出力値は必ず「0」となり、かつANDゲート36aの出力値はQ出力値と同じになるので、乱数出力値はQ出力値と同じになる。すなわち、切替部36の作用により、物理乱数出力値が

「1」であるときは、Q出力値を反転した値が出力乱数となり、逆に物理乱数出力が「0」であるときは、Q出力値がそのまま出力乱数となっている。したがって、本実施形態にかかる乱数生成装置30も、上記実施の形態1と同様に、図2に示した二つの乱数系列(M系列1-1, 1-2)を、物理乱数によって切り替えて出力することができる。すなわち、このような構成によっても、上記実施の形態1と同様の効果が得られる。

#### 【0024】

実施の形態3. 図5は本実施形態にかかる乱数生成装置40の構成図、また図6は、乱数生成装置40によって生成される二つのM系列の巡回パターンを示す図である。乱数生成装置40は、疑似乱数生成部42、物理乱数発生器14、および切替部46を含む。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0025】

本実施形態にかかる疑似乱数生成部42では、線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく二種類の帰還入力値を生成することができる。そして、EXORゲート20bの出力の通過／遮断を物理乱数によって決定している。具体的には、図5の例では、線形シフトレジスタ符号発生器として、シフトレジスタ18と、異なるタップ出力の組み合わせについてそれぞれ排他的論理和を出力する複数のEXORゲート20a, 20b, 20cとが設けられる。EXORゲート20aは、シフトレジスタ18の入力側より第3番目と第17番目のタップ出力(Q3, Q17)の排他的論理和を出力し、EXORゲート20bは、シフトレジスタ18の入力側より第1番目と第2番目のタップ出力(Q1, Q2)の排他的論理和を出力する。EXORゲート20aの出力は直接EXORゲート20cに入力されるが、EXORゲート20bの出力はANDゲート(切替部)46を介してEXORゲート20cに入力される。ANDゲート46には、物理乱数発生器14からの物理乱数出力が入力される。

#### 【0026】

この構成では、物理乱数出力値が「1」である場合には、ANDゲート46の出力値はEXORゲート20bの出力値と同じになるから、EXORゲート20

cからは、シフトレジスタ18への帰還入力値として、EXORゲート20aの出力値とEXORゲート20bの出力値との排他的論理和が出力されることになる。他方、物理乱数出力値が「0」である場合には、ANDゲート46の出力値は必ず「0」となるから、EXORゲート20cからの出力値は、EXORゲート20aの出力値と同じになる。つまり、物理乱数出力値が「0」であるときはタップ出力(Q3, Q17)に基づく帰還入力値が有効となるから、疑似乱数生成部12においてM系列3-1(図6(a))が生成され、他方、物理乱数出力値が「1」であるときは、タップ出力(Q1, Q2, Q3, Q17)に基づく帰還入力値が有効となるから、M系列3-2(図6(b))が生成される。このように、本実施形態にかかる乱数生成装置40も、二つの乱数系列(M系列3-1, 3-2)を、物理乱数によって切り替えて出力することができる。

#### 【0027】

実施の形態4. 図7は本実施形態にかかる乱数生成装置50の構成図、また図8は、乱数生成装置50によって生成される三つのM系列の巡回パターンを示す図である。乱数生成装置50は、疑似乱数生成部52、物理乱数発生器14、および切替部56を含む。なお、ここでは、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0028】

本実施形態にかかる疑似乱数生成部52では、線形シフトレジスタ符号発生器のタップの異なる組み合わせに基づく三種類の帰還入力値を生成することができる。そして、それら三種類の帰還入力値のうちどれを有効とするかを、物理乱数によって決定している。具体的には、図7の例では、線形シフトレジスタ符号発生器として、シフトレジスタ18と、異なるタップ出力の組み合わせに基づく入力値の排他的論理和を出力する複数のEXORゲート20a, 20b, 20c, 20dとが設けられる。EXORゲート20aは、シフトレジスタ18の入力側より第3番目と第17番目のタップ出力(Q3, Q17)の排他的論理和を出力し、EXORゲート20bは、シフトレジスタ18の入力側より第1番目と第2番目のタップ出力(Q1, Q2)の排他的論理和を出力し、またEXORゲート20cは、シフトレジスタ18の入力側より第4番目と第7番目のタップ出力(

Q4, Q7) の排他的論理和を出力する。EXORゲート20aの出力は直接EXORゲート20dに入力されるが、EXORゲート20b, 20cの出力は、それぞれANDゲート56b, 56cおよびORゲート56dを介してEXORゲート20dに入力される。またANDゲート56b, 56cには、三分周器56aからの出力が入力される。

#### 【0029】

本実施形態では、三分周器56a、ANDゲート56b, 56cおよびORゲート56dが、切替部56として機能する。この構成において、公知の構成を有する三分周器56aは、物理乱数発生器14からの物理乱数出力をクロックとして、そのQ1出力値およびQ2出力値を、「0」、「0」(パターン1)、「0」、「1」(パターン2)、「1」、「0」(パターン3)の三パターンで巡回的に更新する。そしてパターン1、すなわちQ1出力値:「0」、Q2出力値:「0」のときは、ORゲート56dの出力値は「0」となり、この場合には、EXORゲート20aの出力値が、シフトレジスタ18に帰還入力値として入力される。同様にパターン2、すなわちQ1出力値:「1」、Q2出力値:「0」のときは、ORゲート56dの出力値は、EXORゲート20bの出力値と同じになる。したがってこの場合には、EXORゲート20dからは、シフトレジスタ18への帰還入力値として、EXORゲート20aの出力値とEXORゲート20bの出力値との排他的論理和が出力される。またパターン3、すなわちQ1出力値「1」、Q2出力値:「0」のときは、ORゲート56dの出力値は、EXORゲート20cの出力と同じ値となる。したがってこの場合には、EXORゲート20dからは、シフトレジスタ18への帰還入力値として、EXORゲート20aの出力値とEXORゲート20cの出力値との排他的論理和が出力される。つまり、物理乱数出力が更新されるたびに、疑似乱数生成部12において、[1] EXORゲート20aに入力されるタップ出力(Q3, Q17)に基づく帰還入力値が有効となるM系列4-1(図8(a))、[2] EXORゲート20a, 20bに入力されるタップ出力(Q1, Q2, Q3, Q17)に基づく帰還入力値が有効となるM系列4-2(図8(b))、および[3] EXORゲート20a, 20cに入力されるタップ出力(Q3, Q4, Q7, Q17)に基づく

帰還入力値が有効となるM系列4-3(図8(c))が生成される。このように、本実施形態にかかる乱数生成装置50は、三つの乱数系列(M系列4-1, 4-2, 4-3)を、物理乱数によって切り替えて出力することができる。

#### 【0030】

実施の形態5. 図9は本実施形態にかかる乱数生成装置60の構成図、また図10は、乱数生成装置60によって生成される二つのM系列の巡回パターンを示す図である。乱数生成装置60は、疑似乱数生成部62、物理乱数発生器14、および切替部66を含む。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0031】

本実施形態にかかる疑似乱数生成部62は、帰還入力を得るタップ(帰還入力の元となるタップ)は同一とし、シフトレジスタのビット数を変更するように構成されており、該シフトレジスタのビット数の変更を物理乱数によって決定している。具体的には、図9の例では、線形シフトレジスタ符号発生器として、15段のシフトレジスタ68と、縦続に配置された二つのフリップフロップ62a, 62bと、所定のタップ出力の組み合わせについて排他的論理和を出力するEXORゲート20eとが設けられる。EXORゲート20eは、シフトレジスタ68の入力側より第1番目と第15番目のタップ出力(Q1, Q15)の排他的論理和を出力する。EXORゲート20eの出力は、前段側のフリップフロップ62aと、ANDゲート66aとに入力される。

#### 【0032】

切替部66は、二つのANDゲート66a, 66bを備えており、そのうち一方のANDゲート66aには、EXORゲート20eの出力と物理乱数発生器14からの物理乱数出力が入力され、もう一方のANDゲート66bには、Q出力と物理乱数発生器14からインバータ66cを介して物理乱数出力が入力される。そして、これら二つのANDゲート66a, 66bの出力がORゲート66dに入力され、このORゲート66dの出力がシフトレジスタ68に入力される。

#### 【0033】

この切替部66により、物理乱数出力に応じて、EXORゲート20eの出力

あるいはフリップフロップ 62b の出力のうちいずれか一方が有効となる。すなわち物理乱数出力値が「0」のときは、ANDゲート 66a の出力値は必ず「0」となり、かつANDゲート 66b の出力値はフリップフロップ 62b の出力値と同じになるから、ORゲート 66d の出力値はフリップフロップ 62b の出力値と同じになる。逆に物理乱数出力値が「1」のときは、ANDゲート 66b の出力は必ず「0」となり、かつANDゲート 66a の出力値はEXORゲート 20e の出力値と同じになるから、ORゲート 66d の出力値はEXORゲート 20e の出力値と同じ値となる。すなわち、切替部 66 の作用により、物理乱数出力値が「0」であるときは、フリップフロップ 62a, 62b もシフトレジスタの一部として機能することになり、これらを含めた 17 段のシフトレジスタによって、タップ出力 (Q3, Q17) に基づく帰還入力値が有効となる M 系列 5-1 (図 10 (a)) が生成される。他方、物理乱数出力が「1」であるときは、フリップフロップ 62a, 62b は無効となり、15 段のシフトレジスタ 68 によって、タップ出力 (Q1, Q15) に基づく帰還入力値が有効となる M 系列 5-2 (図 10 (b)) が生成される。このように、本実施形態にかかる乱数発生装置 60 は、段数の異なる二つのシフトレジスタによって発生される乱数系列 (M 系列 5-1, 5-2) を、物理乱数によって切り替えて出力することができる。

#### 【0034】

実施の形態 6. 図 11 は本実施形態にかかる乱数生成装置 70 の構成図である。乱数生成装置 70 は、疑似乱数生成部 72、物理乱数発生器 14、および切替部 16 を含む。本実施形態の疑似乱数生成部 72 は、シフトレジスタ 78 (18) 内に後述する検出回路 78a が設けられている点を除いては実施の形態 1 の疑似乱数生成部 12 と同じであり、図 2 に示す M 系列 1-1, 1-2 を生成することができる。なお、ここでも、上記実施形態と同じ構成要素については同じ符号を付し、重複する部分の説明は省略する。

#### 【0035】

線形シフトレジスタ符号発生器は、シフトレジスタ内の符号列によっては、M 系列符号を生成できない。例えば、シフトレジスタの全ビットの値が「0」であ

る場合にはM系列1-1を生成することができないし、また、シフトレジスタの全ビットが「1」である場合にはM系列1-2を生成することができない。一の疑似乱数系列の符号のみを生成する従来の一般的な線形シフトレジスタ符号発生器では、例えば初期値をそのような符号列としないように留意すれば十分であったが、上記実施形態のように、生成される疑似乱数系列が動作中に変更される場合には、有効な疑似乱数系列に対してシフトレジスタ内の符号列が該系列を生じないものとならないようにするための対策を講じておくのが望ましい。そのために、本実施形態にかかる乱数生成装置70は、上記実施の形態1にかかる乱数生成装置10に、検出回路78a、78b、ANDゲート82a、82b、フリップフロップ84a、84b、およびフリップフロップ80を付加した構成となっている。

#### 【0036】

上記付加的な構成要素について説明する。物理乱数発生器14からの出力（物理乱数出力）は、フリップフロップ80に入力される。なお、本実施形態でも、物理乱数出力値「0」はM系列1-1（図2（a））を、また「1」はM系列1-2（図2（a））を示すものとして規定されている。検出回路78aは、シフトレジスタ78の全ビットの値が「1」であるときに、ANDゲート82aに「1」を出力する（例えば全ビットの値の論理積を出力する）。また検出回路78bは、シフトレジスタ78の全ビットの値が「0」であるときに、ANDゲート82bに「1」を出力する（例えば全ビットの反転値の論理積を出力する）。ANDゲート82aには、検出回路78aの出力とフリップフロップ80のQ出力とが入力され、その出力はフリップフロップ84aに入力される。ANDゲート82bには、検出回路78bの出力とフリップフロップ80のQb出力とが入力され、その出力はフリップフロップ84bに入力される。そして、フリップフロップ84aの出力はリセット信号（R入力）として、またフリップフロップ84bの出力はセット信号（S入力）として、フリップフロップ80に入力される。なお、図11の例では、検出回路78a、78bはシフトレジスタ78に内蔵されているが、これらをシフトレジスタ78の外部に接続してもよい。

#### 【0037】

上記構成において、シフトレジスタ78の全ビットの値が「1」であるときに、物理乱数出力値が「0」から「1」に変化すると、フリップフロップ80の値は「1」となり、Q出力値が「1」となる。また、検出回路78aの出力値は「1」であるから、ANDゲート82aの出力値は「1」となる。そして、フリップフロップ84aの値が「1」となって、フリップフロップ80にリセット信号が入力される。したがって、この場合、フリップフロップ80の値は「1」から「0」に変更される。すなわち上記構成によれば、シフトレジスタ78においてM系列1-1（図2（a））の符号が生じない状態（すなわち全ビットの値が「0」）となるのを防止することができる。

#### 【0038】

一方、シフトレジスタ78の全ビットの値が「0」であるときに、物理乱数出力値が「1」から「0」に変化すると、フリップフロップ80の値が「0」となり、Qb出力値が「1」となる。また、検出回路78bの出力値は「1」であるから、ANDゲート82bの出力値は「1」となる。そして、フリップフロップ84bの値が「1」となって、フリップフロップ80にセット信号が入力される。したがって、この場合、フリップフロップ80の値は「0」から「1」に変更される。すなわち上記構成によれば、シフトレジスタ78においてM系列1-2（図2（b））の符号が生じない状態（すなわち全ビットの値が「1」）となるのを防止することができる。

#### 【0039】

なお、フリップフロップ84a、84bの出力により、シフトレジスタ78の少なくとも一つのビットの値を変化させるようにしても同様の効果が得られる。例えば、フリップフロップ84aの出力を、シフトレジスタ78内を構成する少なくとも一つのフリップフロップのリセット信号とすれば、当該フリップフロップ（ビット）の値が「0」となるので、M系列1-1の符号を生じない状態となるのを防止することができる。また、フリップフロップ84bの出力をシフトレジスタ78内を構成するいずれかのフリップフロップのリセット信号とすれば、当該フリップフロップ（ビット）の値が「1」となるので、M系列1-2の符号を生じない状態となるのを防止することができる。

## 【0040】

以上、本発明の好適な実施形態について説明したが、本発明は上記実施形態で示した構成には限定されず、種々の等価回路によっても実施可能である。上記実施形態では、疑似乱数が、17段または15段のシフトレジスタを有する線形シフトレジスタ符号発生器によって生成される数種類のM系列符号である場合を例示したが、これには限定されず、それ以外の段数のシフトレジスタあるいはタップの組み合わせに基づくM系列であってもよい。また、上記実施の形態6は、上記実施の形態1を基礎としたものを例示的に示したが、他の実施形態に対しても同様に適用可能であることは言うまでもない。また、上記実施の形態1, 3～6では、シフトレジスタの最終段のフリップフロップからの出力を乱数出力としたが、他のフリップフロップからの出力を乱数出力としてもよいし、シフトレジスタに入力される帰還値を乱数出力としてもよい。

## 【0041】

## 【発明の効果】

本発明によれば、複数の疑似乱数系列のうちどれを有効とするかを物理乱数によって切り替えるため、その予測が難しく暗号化アルゴリズム等への適用に際してより安全性の高い乱数を生成することができる。

## 【図面の簡単な説明】

【図1】 本発明の実施の形態1にかかる乱数生成装置の構成図である。

【図2】 本発明の実施の形態1にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

【図3】 本発明の実施の形態にかかる物理乱数発生器の構成図である。

【図4】 本発明の実施の形態2にかかる乱数生成装置の構成図である。

【図5】 本発明の実施の形態3にかかる乱数生成装置の構成図である。

【図6】 本発明の実施の形態3にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

【図7】 本発明の実施の形態4にかかる乱数生成装置の構成図である。

【図8】 本発明の実施の形態4にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

【図 9】 本発明の実施の形態 5 にかかる乱数生成装置の構成図である。

【図 10】 本発明の実施の形態 5 にかかる乱数生成装置によって生成される疑似乱数系列の一例を示す図である。

【図 11】 本発明の実施の形態 6 にかかる乱数生成装置の構成図である。

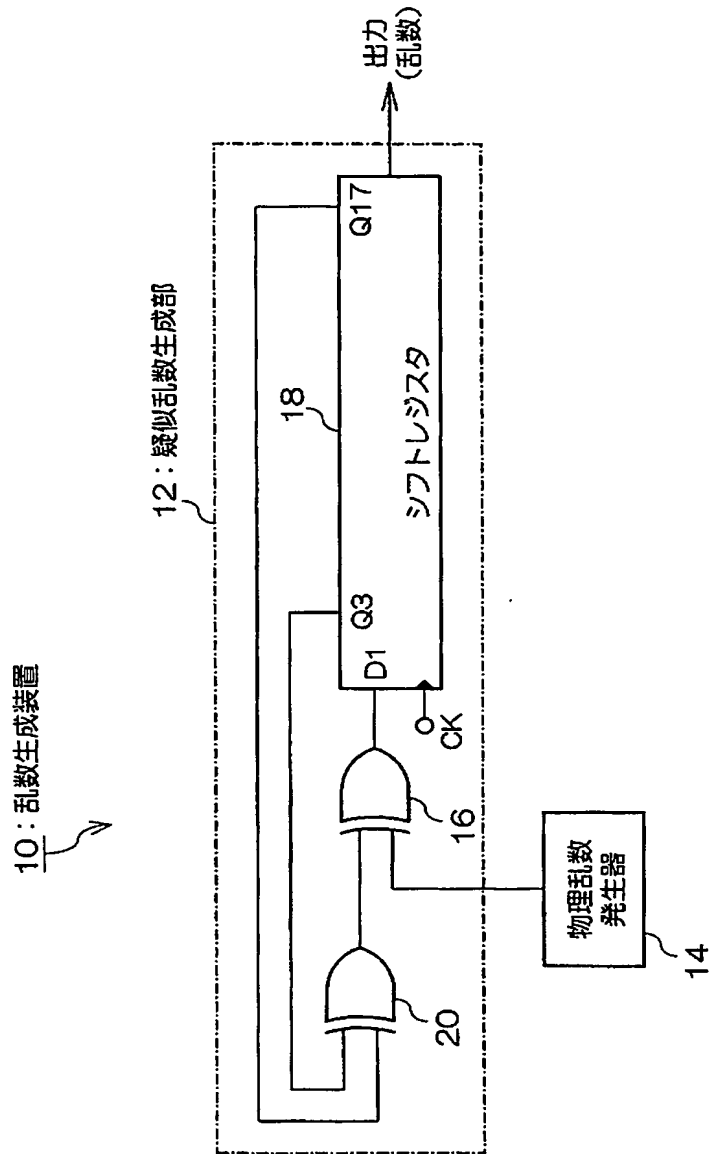
【符号の説明】

10, 30, 40, 50, 60, 70 乱数生成装置、12, 32, 42, 52, 62, 72 疑似乱数生成部、14 物理乱数発生器、16, 36, 46, 56, 66 切替部、18, 78 シフトレジスタ、20, 20a, 20b, 20c, 20d, 20e EXORゲート、62a, 62b フリップフロップ、78a, 78b 検出回路。

【書類名】

図面

【図 1】



【図 2】

(a)

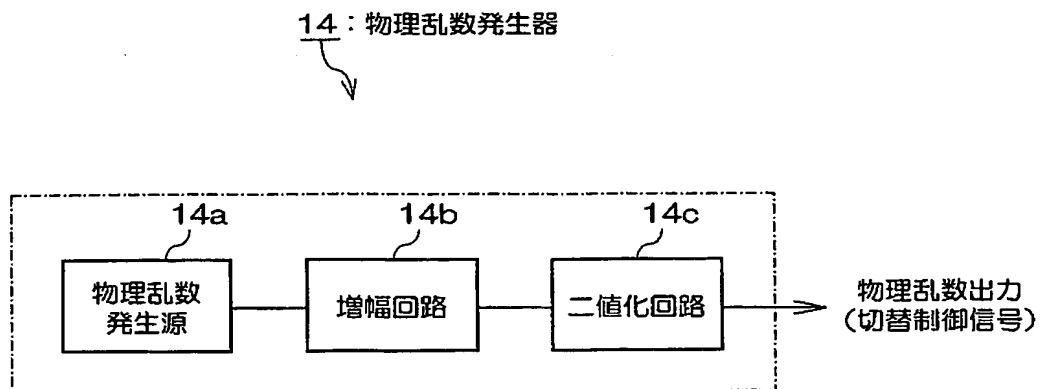
M系列1-1 (物理乱数: 0)		1	2	3	4	FF	5	...	16	17
タイミング	t(1)	1	1	1	1	1	1	...	1	1
	t(2)	0	1	1	1	1	1	...	1	1
	t(3)	0	0	1	1	1	1	...	1	1
	t(4)	0	0	0	1	1	1	...	1	1
	t(5)	1	0	0	0	1	1	...	1	1
	t(6)	1	1	0	0	0	0	...	1	1
	...			...					...	
	t(2 <sup>17</sup> -1)	1	1	1	1	1	1	...	1	0



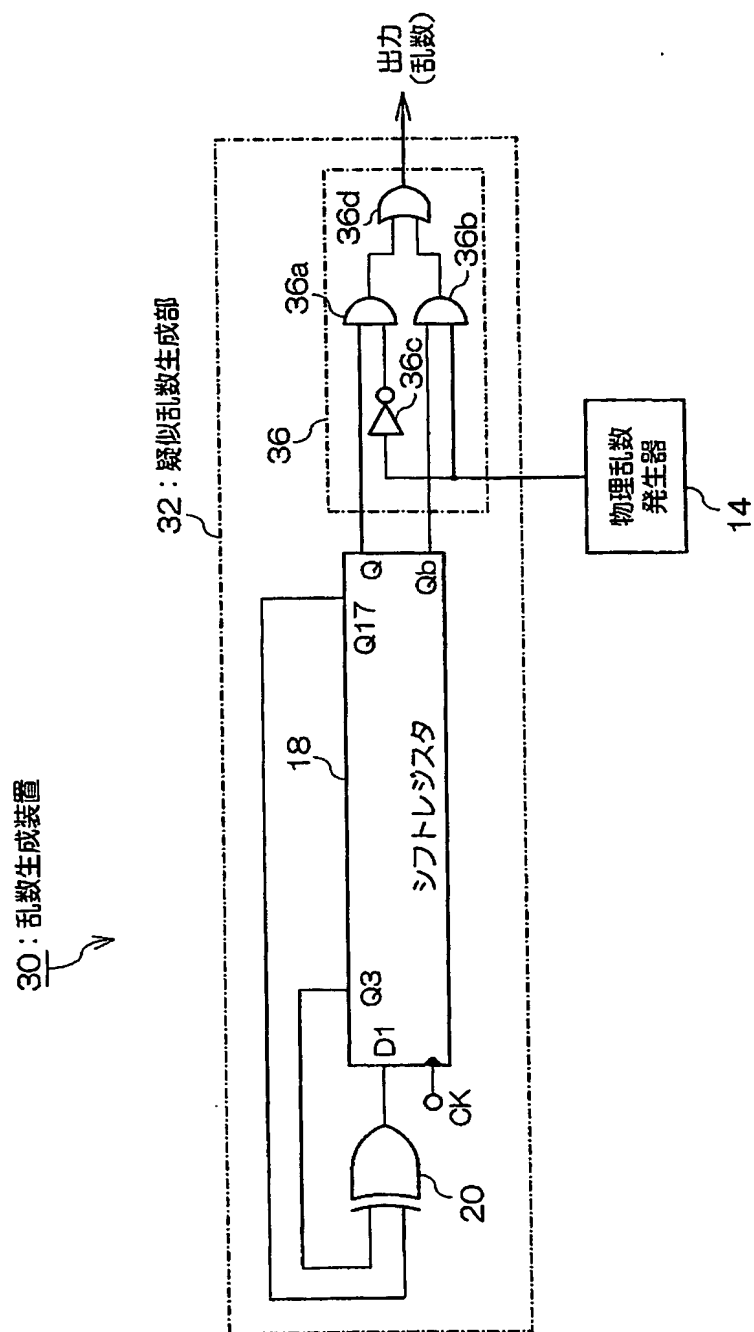
(b)

M系列1-2 (物理乱数: 1)		1	2	3	4	FF	5	...	16	17
タイミング	t(1)	0	0	0	0	0	0	...	0	0
	t(2)	1	0	0	0	0	0	...	0	0
	t(3)	1	1	0	0	0	0	...	0	0
	t(4)	1	1	1	0	0	0	...	0	0
	t(5)	0	1	1	1	0	0	...	0	0
	t(6)	0	0	1	1	1	1	...	0	0
	...			...					...	
	t(2 <sup>17</sup> -1)	0	0	0	0	0	0	...	0	1

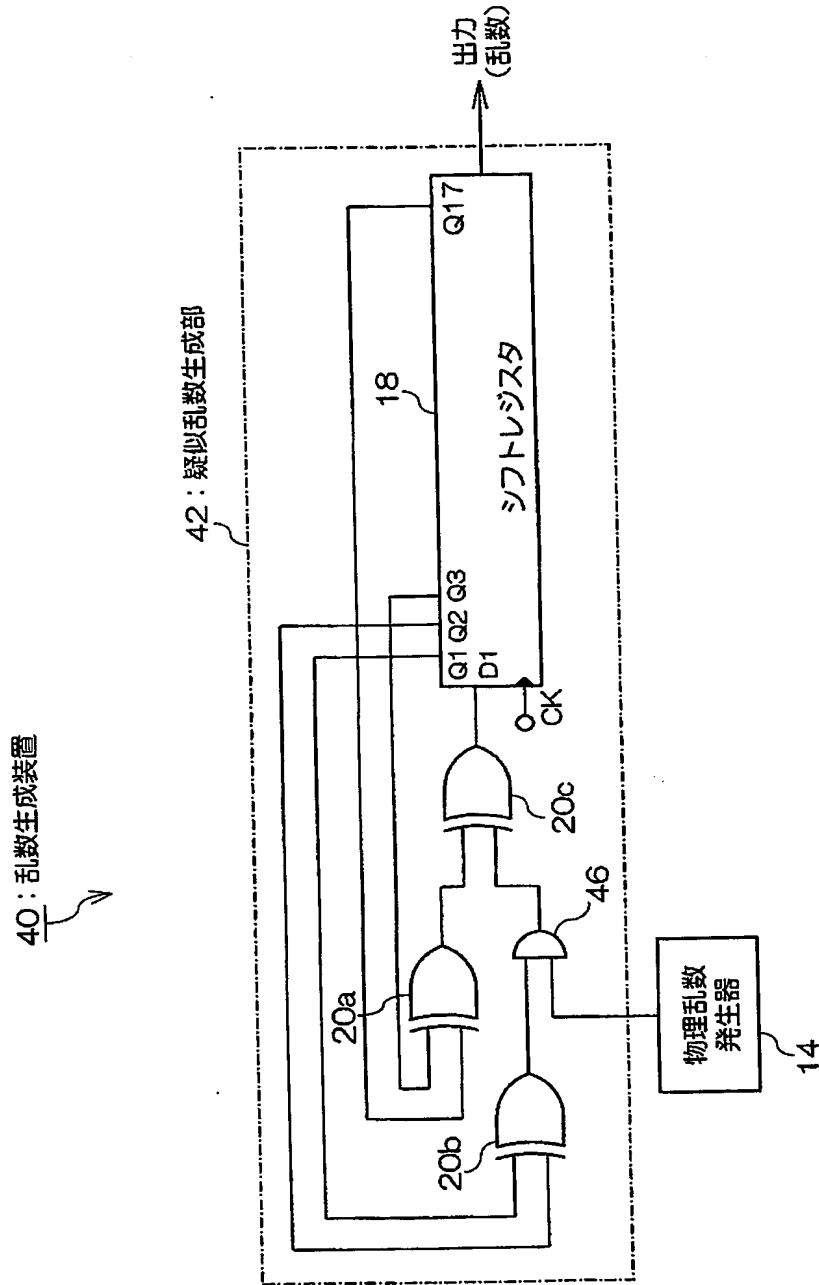
【図 3】



【図 4】



【図 5】



【図 6】

(a)

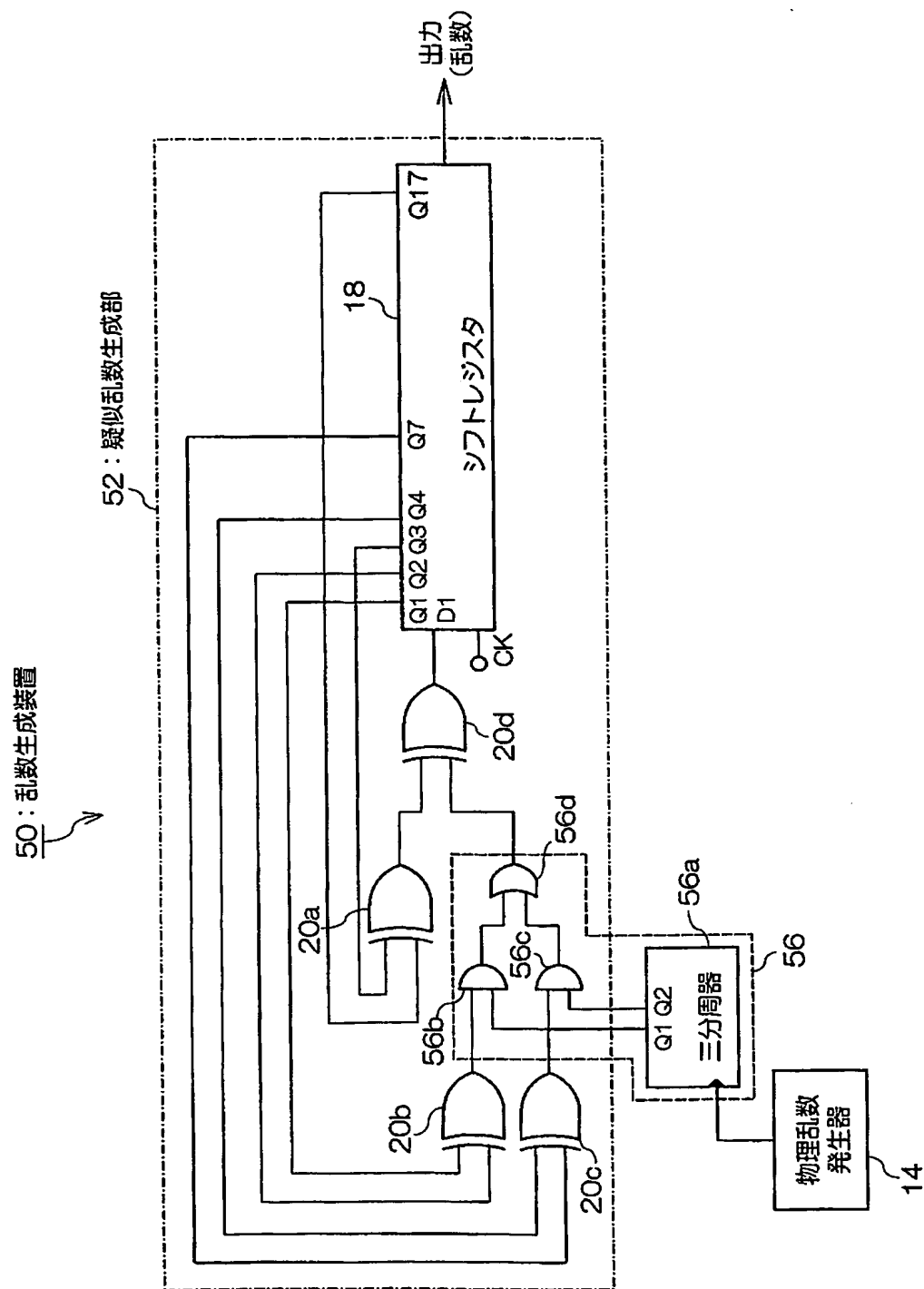
M系列3-1 (物理乱数: 0)		1	2	3	4	FF 5	...	16	17
タイミング	t(1)	1	1	1	1	1	...	1	1
	t(2)	0	1	1	1	1	...	1	1
	t(3)	0	0	1	1	1	...	1	1
	t(4)	0	0	0	1	1	...	1	1
	t(5)	1	0	0	0	1	...	1	1
	t(6)	1	1	0	0	0	...	1	1
	...			...				...	
	t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0



(b)

M系列3-2 (物理乱数: 1)		1	2	3	4	FF 5	...	16	17
タイミング	t(1)	1	1	1	1	1	...	1	1
	t(2)	0	1	1	1	1	...	1	1
	t(3)	1	0	1	1	1	...	1	1
	t(4)	0	1	0	1	1	...	1	1
	t(5)	0	0	1	0	1	...	1	1
	t(6)	1	0	0	1	0	...	1	1
	...			...				...	
	t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0

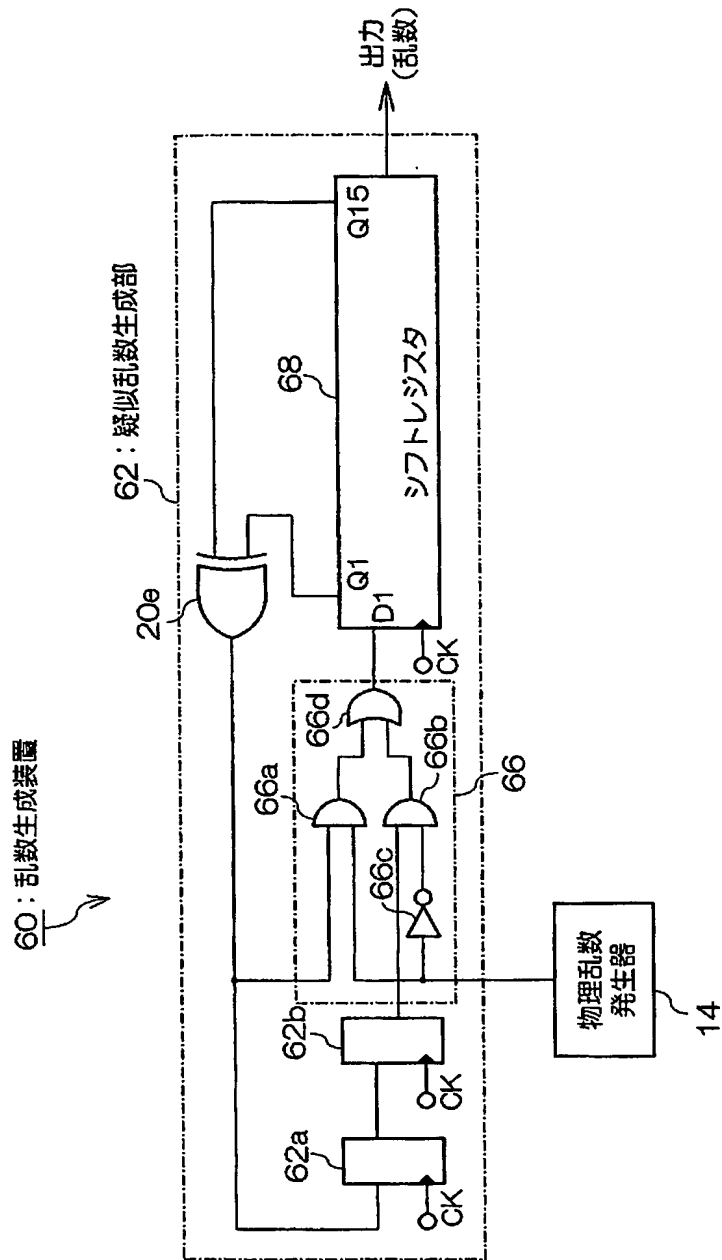
【図 7】



【図 8】

		M系列4-1 (Q1=0,Q2=0)		FF					
		1	2	3	4	5	...	16 17	
(a)	タイミング	t(1)	1	1	1	1	1	...	1 1
		t(2)	0	1	1	1	1	...	1 1
		t(3)	0	0	1	1	1	...	1 1
		t(4)	0	0	0	1	1	...	1 1
		t(5)	1	0	0	0	1	...	1 1
		t(6)	1	1	0	0	0	...	1 1
		⋮			⋮				⋮
		t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1 0
		M系列4-2 (Q1=1,Q2=0)		FF					
		1	2	3	4	5	...	16 17	
(b)	タイミング	t(1)	1	1	1	1	1	...	1 1
		t(2)	0	1	1	1	1	...	1 1
		t(3)	1	0	1	1	1	...	1 1
		t(4)	0	1	0	1	1	...	1 1
		t(5)	0	0	1	0	1	...	1 1
		t(6)	0	0	0	1	0	...	1 1
		⋮			⋮				⋮
		t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1 0
		M系列4-3 (Q1=0,Q2=1)		FF					
		1	2	3	4	5	...	16 17	
(c)	タイミング	t(1)	1	1	1	1	1	...	1 1
		t(2)	0	1	1	1	1	...	1 1
		t(3)	0	0	1	1	1	...	1 1
		t(4)	0	0	0	1	1	...	1 1
		t(5)	1	0	0	0	1	...	1 1
		t(6)	0	1	0	0	0	...	1 1
		⋮			⋮				⋮
		t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1 0

【図 9】



【図 10】

(a)

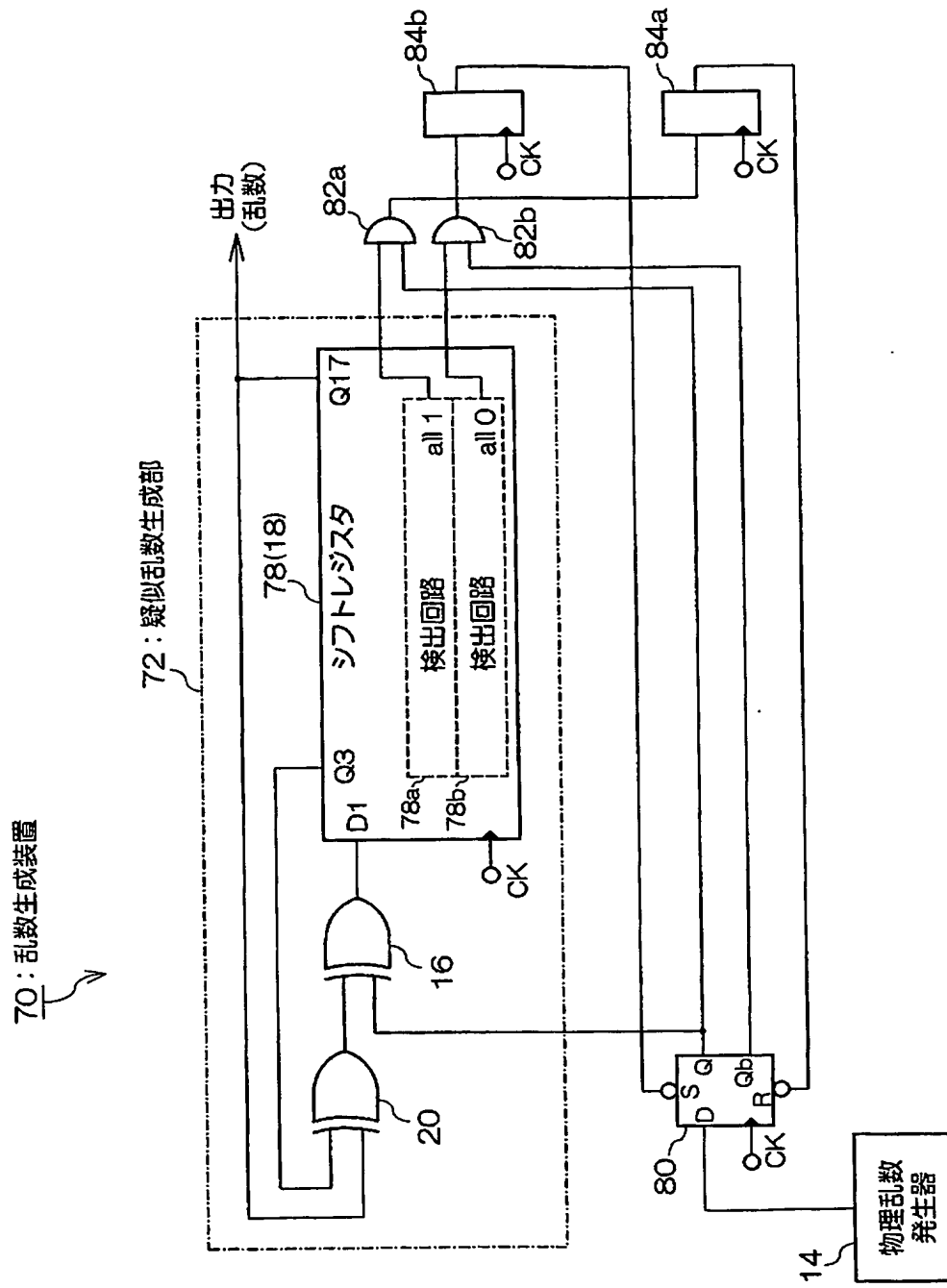
M系列5-1 (物理乱数:0)		1	2	3	4	FF 5	...	16	17
タイミング	t(1)	1	1	1	1	1	...	1	1
	t(2)	0	1	1	1	1	...	1	1
	t(3)	0	0	1	1	1	...	1	1
	t(4)	0	0	0	1	1	...	1	1
	t(5)	1	0	0	0	1	...	1	1
	t(6)	1	1	0	0	0	...	1	1
	...			...				...	
	t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0



(b)

M系列5-2 (物理乱数:1)		1	2	3	4	FF 5	...	14	15
タイミング	t(1)	1	1	1	1	1	...	1	1
	t(2)	0	1	1	1	1	...	1	1
	t(3)	1	0	1	1	1	...	1	1
	t(4)	0	1	0	1	1	...	1	1
	t(5)	1	0	1	0	1	...	1	1
	t(6)	1	1	0	1	0	...	1	1
	...			...				...	
	t(2 <sup>17</sup> -1)	1	1	1	1	1	...	1	0

【図 11】



【書類名】 要約書

【要約】

【課題】 暗号化アルゴリズム等に用いられる乱数生成装置において、より安全性の高い乱数を生成する。

【解決手段】 乱数生成装置 10 は、複数の異なる疑似乱数系列の乱数を出力可能な疑似乱数生成部 12 と、物理乱数を生成する物理乱数発生器 14 と、物理乱数発生器 14 の生成した物理乱数に基づいて疑似乱数生成部 12 の出力する乱数の疑似乱数系列を切り替える切替部 16 と、を備え、疑似乱数生成部 12 の出力を出力乱数とする。複数の異なる疑似乱数系列を物理乱数によって切り替えて出力するため、従来の疑似乱数のみを用いた乱数生成装置に比べて乱数の予測性を低減することができる。また、物理乱数を直接的な出力乱数としては用いないため、仮に外部から物理乱数生成手段に何らかの操作が加えられたとしても、出力乱数の予測性に対する影響は従来装置に比べてかなり小さくなる。

【選択図】 図 1

特願 2002-320035

出 願 人 履 歴 情 報

識別番号

[000001889]

1. 変更年月日

1993年10月20日

[変更理由]

住所変更

住 所

大阪府守口市京阪本通2丁目5番5号

氏 名

三洋電機株式会社

特願 2002-320035

出 願 人 履 歴 情 報

識別番号

[502398610]

1. 変更年月日

2002年11月 1日

[変更理由]

新規登録

住 所

群馬県前橋市上佐鳥町54-2

氏 名

株式会社数理設計研究所

特願 2002-320035

出 願 人 履 歴 情 報

識別番号

[502343458]

1. 変更年月日

2002年 9月20日

[変更理由]

新規登録

住 所

東京都台東区上野1丁目19番10号

氏 名

三洋セミコンデバイス株式会社